Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.4, No.7, 2014

Point - to - Point Virtual Private Network Based on IP Filtering and Rijndael Encryption Algorithm

Eng.Nedhal Ahmad Hamdi
Iraqi Commission for Computers and Informatics,
Informatics Institute for Postgraduate Studies
Hay Al Nasser, Kirkuk, Iraq
Tel: 00-964-7704009094 E-mail: nedhal.ahmad @yahoo.com

Prof. Dr. Eng. *Imad Hussain AL. Hussaini*
Baghdad-Iraq

1. Abstract

The Rijndael algorithm was chosen to take advantage of its features and add recent technology to increase the confidentiality and security for the transfer of sensitive data on some important institutions. Rijndael algorithm (Advance Encryption Standard) is the Encryption of Symmetric Key, each one of the keys has size of 128 bit. Each round consists of several processing steps; one of them is depend on the encryption key. Therefore NEDRO program has been designed depending on Rijndael algorithm and updated by adding the key (Initialization Vector), in addition to taking into consideration the possibilities that could face the process of transmission of data between two sides. Finally NEDRO program has implemented and tested practically between two points (User making encryption and Host making decryption or Host making encryption and User making decryption at the same time)

Keywords : Cryptography , Rijndael (AES) ,Data Security , Encryption , Decryption

2. Introduction

Cryptography is the science of information and communication security. Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against unauthorized parties by preventing unauthorized alteration of use. It uses a cryptographic system to transform a plaintext into a cipher text, using most of the time a key [1][2]. There exists certain cipher that doesn't need a key at all. The Rijndael is the winner of the contest, held in 1997 by the US Government, after the Data Encryption Standard (DES) was found too weak because of its small key size and the technological advancements in processor power [3].

In October 2000, one of these five algorithms was selected as the forthcoming standard: a slightly modified version of the Rijndael. The Rijndael, whose name is based on the names of its two Belgian inventors, Joan Daemen and Vincent Rijmen, is a block cipher, which means that it works on fixed-length group of bits, which are called blocks. It takes an input block of a certain size, usually 128, and produces a corresponding output block of the same size. The transformation requires a second input, which is the secret key. It is important to know that the secret key can be of any size [4]. In modern ages, cryptography development has been a major concern in the fields of mathematics, computer science and engineering. One of the main classes in cryptography today is the symmetric-key cryptography, where a shared key of a certain size will be used for the encryption and decryption processes [5].

Cryptography is the science of information and communication security. Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against

unauthorized parties by preventing unauthorized alteration of use. It uses a cryptographic system to transform a plaintext into a cipher text, using most of the time a key [7]. There exists certain cipher that doesn't need a key at all. The Rijndael is the winner of the contest, held in 1997 by the US Government, after the Data Encryption Standard (DES) was found too weak because of its small key size and the technological advancements in processor power [8].

In October 2000, one of these five algorithms was selected as the forthcoming standard: a slightly modified version of the Rijndael. The Rijndael, whose name is based on the names of its two Belgian inventors, Joan Daemen and Vincent Rijmen, is a block cipher, which means that it works on fixed-length group of bits, which are called blocks. It takes an input block of a certain size, usually 128, and produces a corresponding output block of the same size. The transformation requires a second input, which is the secret key. It is important to know that the secret key can be of any size [9]. In modern ages, cryptography development has been a major concern in the fields of mathematics, computer science and engineering. One of the main classes in cryptography today is the symmetric-key cryptography, where a shared key of a certain size will be used for the encryption and decryption processes [10].

3. Virtual Private Networks (VPN)

Secure transfer of data in network or internet depends on safe way to transfer data from place to other after encrypting them therefore (VPN) has been chosen

- A VPN is a private connection between two or more network elements over a shared (typically public network) infrastructure. The "virtual" defines a logical definition between the networks, not a separate physical network[11]. The "private" defines separate addressing and routines. It typically uses encryption and tunneling to achieve one or more aims therefore this way satisfies safe provision of private communications within the public Internet Infrastructure and applies various networking technologies to achieve the goal [12] .

- Is a tool for protecting personal information such as financial information, login information, passwords etc from being accessed by others. Internet Encryption Software uses a technique called cipher text to transform data into codes and symbols that are not understood and cannot be read by other users [13].

4- The Rijndael(Advanced Encryption Standard-AES)

(AES) was announced by National Institute of Standards and Technology (NIST) as on November 26, 2001 after a 5-year standardization process in which fifteen competing designs were presented and evaluated before Rijndael was selected as the most suitable [14]. It became effective as a standard May 26, 2002. As of 2009, AES is one of the most popular algorithms used in symmetric key cryptography .It is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the NSA for top secret information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits using cipher keys with lengths of 128, 192 and 256 –bits [15].

The AES specifies a cryptographic algorithm that can be used to protect electronic data. The AES algorithm is asymmetric block cipher that can encrypt and decrypt information. Encryption converts data to an unknown form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext. It can widely be used for electronic commerce, secure communication. Computational efficiency: The evaluation of computational efficiency will be applicable to both hardware and Software implementations [16].

5- Rijndael Encryption and Decryption Algorithms

- The choice was based on a careful and comprehensive analysis of the security and efficiency characteristics of Rijndael's algorithm. Rijndael is an iterated block cipher .Therefore, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function) also it defines a method to generate a series of sub keys from the original key. The generated sub keys are used as input with the round function [17].

- The primary focus of the analysis is on the cipher's security, but the choice of Rijndael was based on its simple algorithm and implementation characteristics. There were several candidate algorithms but Rijndael was selected because based on the analysis, it has the best combination of security, performance, efficiency, ease of implementation and flexibility[18] as shown in Figure (1.1).

- The decryption process is the exact inverse of encryption. The inverses of the transformations are done from the starting with the inverse of the final round. In the Inverse ByteSub Transformation, inverse S-boxes are used. In the Inverse ShiftRow Transformation, cyclically shifting is done to the right with the same offsets of the ShiftRow Transformation. The Inverse MixColumn Transformation is more complicated than then the MixColumn Transformation as shown in Figure (1.2)[19].

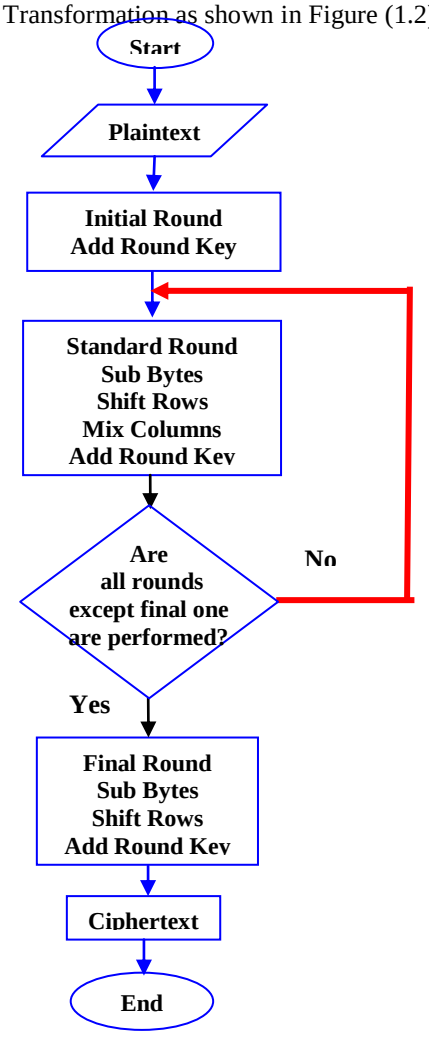

Figure (1.1). Rijndael Encryption Algorithm Algorithm

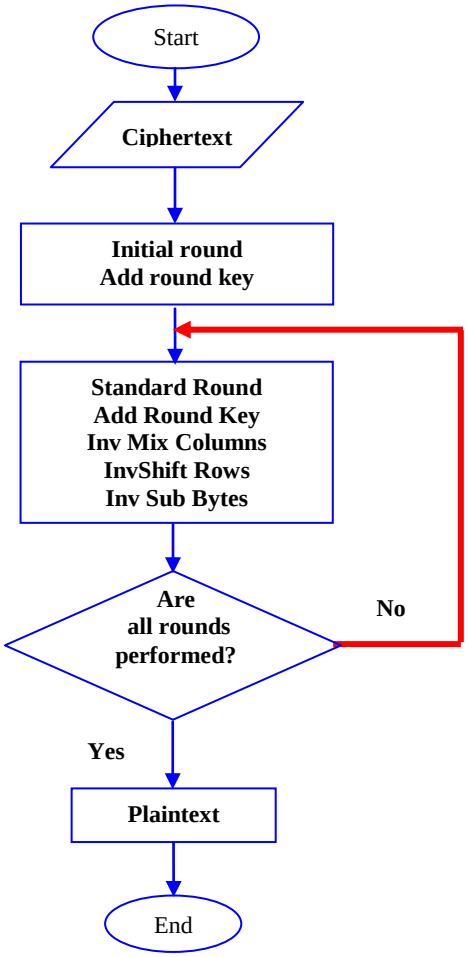

Figure (1.2) Rijndael Decryption

6. Add Initialization Vector (IV)

- An initialization vector (IV) is a random value that changes with every instance of the cipher that is used to add some randomness to the output of the cipher. Since this value is random and unique, it makes the output of the stream cipher safer than other outputs, even if the same key is used. This is useful when key exchange is expensive. It is important to recognize the proper role of the IV. In this kind of usage, the initialization vector is not part of the secret key, and does not need to be kept secret. This means that it can be transmitted in the clear to the recipient. However, making sure it is random can help prevent pre computation-based [20].

To the first 256 bits of the hashed byte to create the key, then use the next 128 bits of our hashed byte to create the IV. This function is almost identical to the previous one.

```
Private  Function  As  Byte (  )
  Dim bytIV As Byte( )
        Byte [] IV = {0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x10, 0x11, 0x12, 0x13, 0x14, 0x15,
      0x16};
  Return bytIV 'Return the IV.
End Function
```

- Cipher Block Chaining Mode in ENDRO Program

That same plaintext blocks produce different cipher text blocks. Cipher Block Chaining allows this by XORing each plaintext with the cipher text from the previous round (the first round using an Initialization Vector (IV)). As before, the same key is used for each block. Decryption works because of the properties of the XOR operation[21].

7. NEDRO Encryption Algorithm

The managed symmetric cryptography classes are used with a special stream class called a *CryptoStream* that encrypts data read into the stream. The *CryptoStream* class is initialized with a managed stream class, a class implements the *ICryptoTransform* interface (created from a class that implements a cryptographic algorithm), and a *CryptoStream* Mode enumeration that describes the type of access permitted to the *CryptoStream*. The *CryptoStream* class can be initialized using any class that is derived from the Stream class, including Data Stream, *MemoryStream*, and. Net work Stream.

Also shown a new instance of the *RijndaelManaged* class is created, which implements the Rijndael encryption algorithm, and uses it to perform encryption on a *CryptoStream* class. The *CryptoStream* is initialized with a stream object called *MyStream* that can be any type of managed stream. The *CreateEncryptor* method from the *RijndaelManaged* class is passed the key and IV that are used for encryption. In this case, the default key and IV are generated. Finally the *(CryptoStream)* Mode. Write is passed, specifying write access to the stream as shown in Figure (1.3).

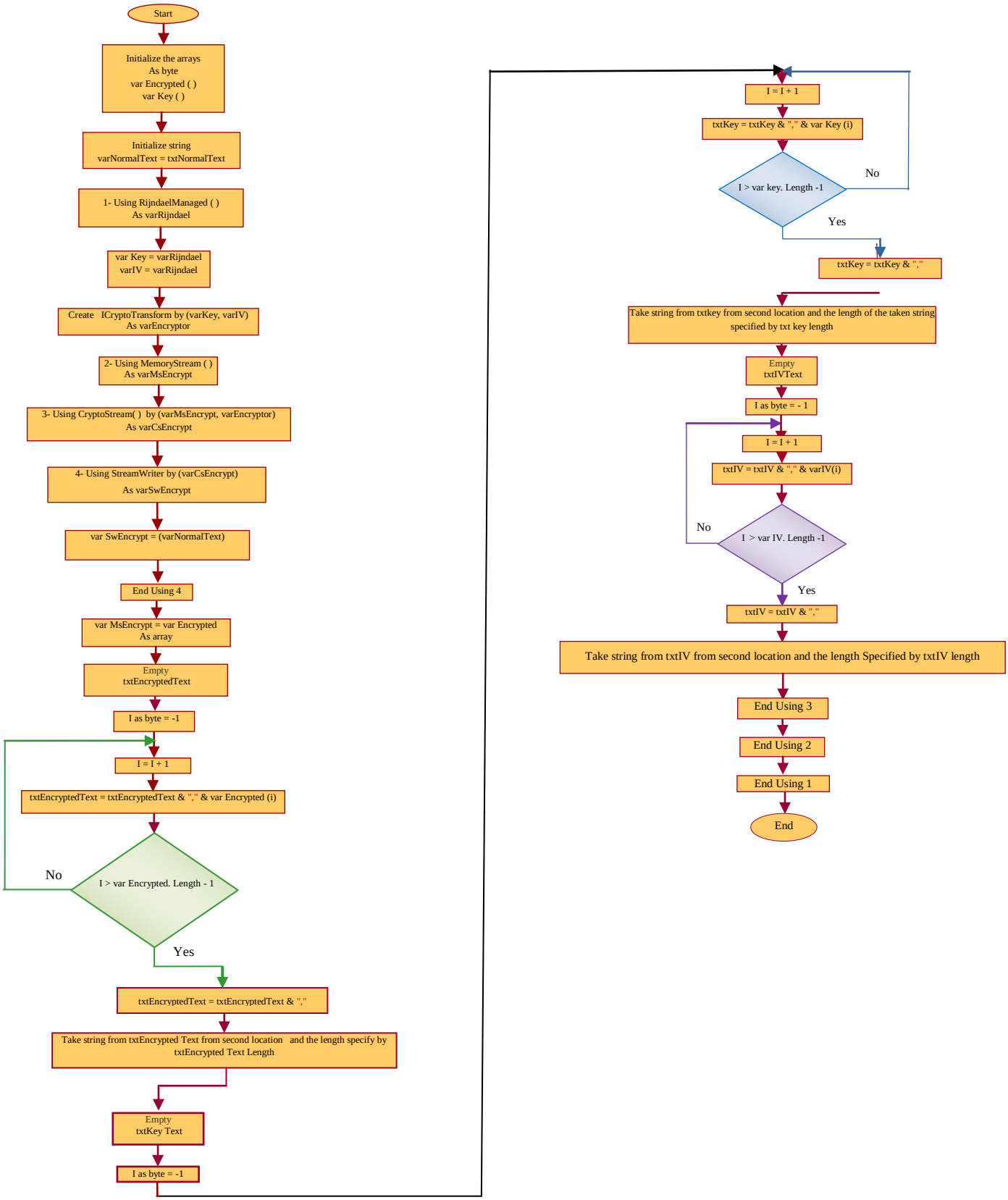

Figure (1.3). NEDRO Encryption Algorithm

8. NEDRO Decryption Algorithm

The *CryptoStream* class is used with symmetric cryptography classes decrypt data read from any managed stream.

Also shown a new instance of the *RijndaelManaged* class is created and used it to perform decryption on a *CryptoStream* object. At first a new instance of the *RijndaelManaged* class is created. Next it creates a *CryptoStream* object and initializes it to the value of a managed stream called *MyStream*. Next, the Create Decryptor method from the *RijndaelManaged* class is passed the same key and IV that was used for encryption and is then passed to the *CryptoStream* constructor. Finally, the *CryptoStream* Mode .Read enumeration is passed to the *CryptoStream* constructor to specify read access to the stream as shown in Figure (1.4).

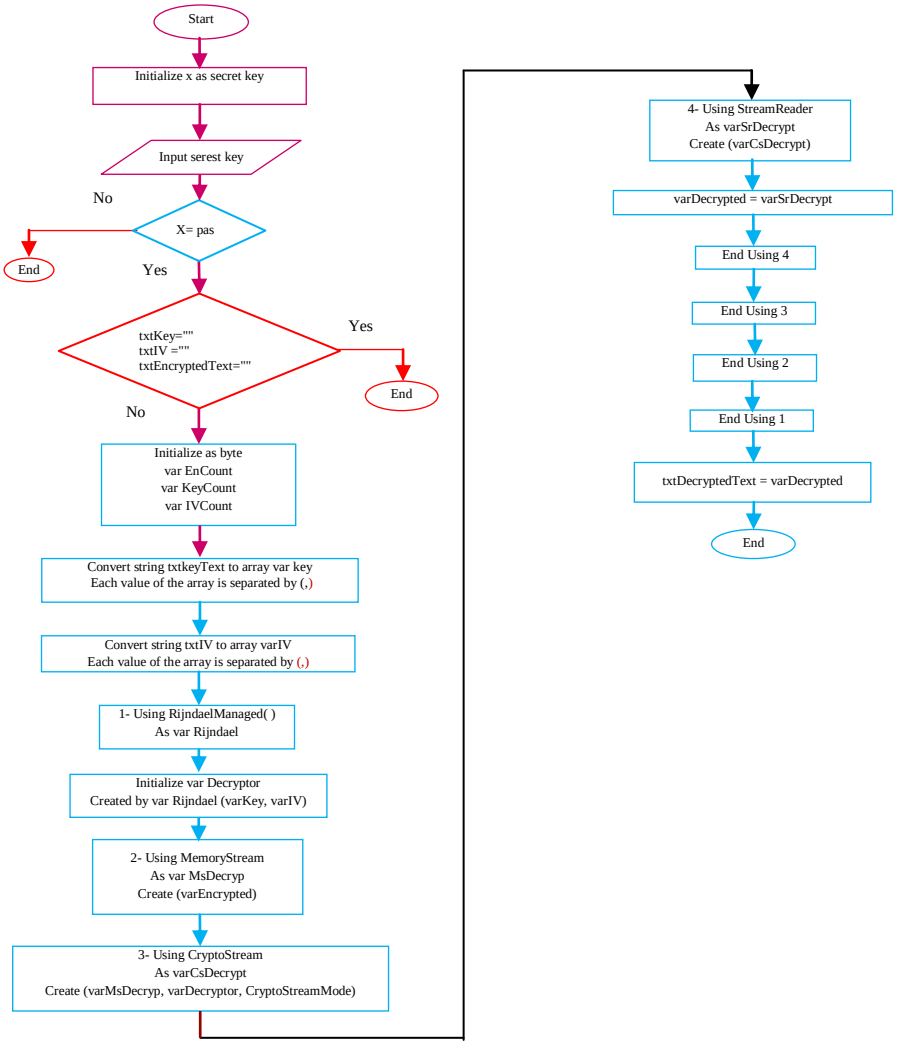

Figure (1.4). NEDRO Decryption Algorithm

9- NEDRO Program

This Program includes three stages, *first*, Program Code writing, *second*, design interface of the program, *third*, operating the program

Design of the program involves making encryption one stage (NEDRO Program) by using Visual Studio.Net 2010. It provides namespace *(System.Security.Cryptography)* in Visual Sudio.Net variety of tools assist in the encryption and decryption. *(CryptoStream)* class is one of the many classes that are provided *(CryptoStream)* class is used to encrypt or decrypt content as streaming content out to the file.Finally NEDRO program is implemented with real data and generation map as shown in Figure (1.5) and its interface shown in Figure (1.6).

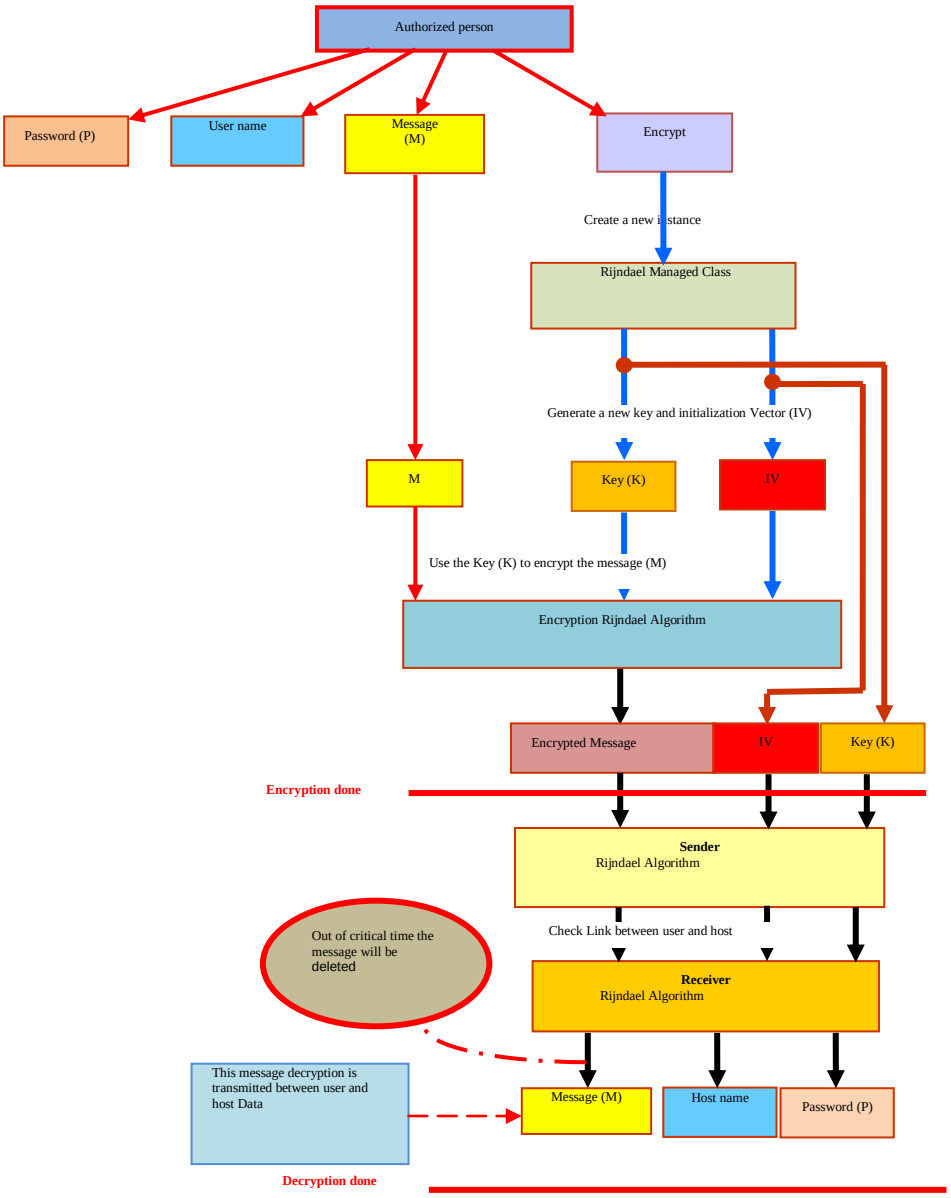

Figure (1.5). generation map

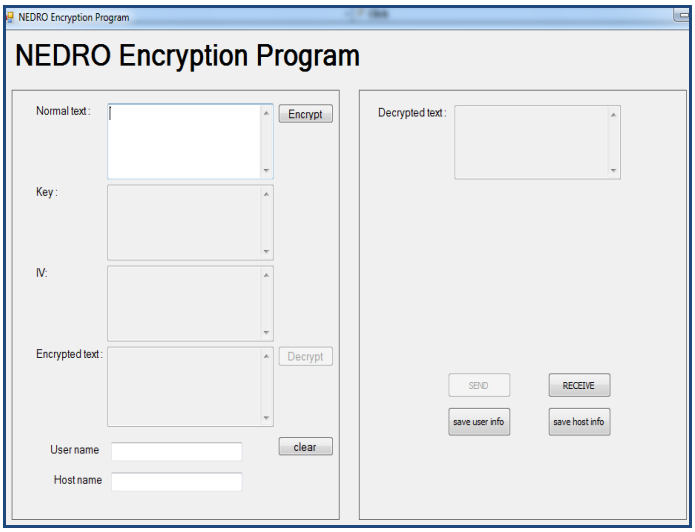

Figure (1.6) NEDRO Program Interface.

10. Conclusions:

1- Using 10 rounds for Rijndael algorithm in this thesis has increased security level by 85% because adding key to the first round leads to decrease in the decrypted probability in each round.

2- Using of an IV prevents repetition in data encryption, making it very difficult for a hacker using a dictionary (ASCII code) attack to find patterns and break a cipher.

3- A proposed algorithm is introduced to generate IV from cipher key by changing only two bits of cipher key to generate new KEY.

4- A proposed algorithm makes many S-Boxes by changing Cipher key. That means increase in speed and satisfying good performance, (two languages and all symbols and numbers) of NEDRO program generation.

5- The work has been done on technique of (Encryption by designing software) to get 100% security against all kinds of side channel attacks.

11. Suggestions for Future Work

1- Developing NEDRO Program by adding some procedures to make it usable in communication in Mobile Technology and increase its messages security.

2- In this work size of 128 bit is used but in future it must be developed to use size of 192 bit for increasing size of the key.

3- NEDRO Program may be used in Smart Cards in future by adding some functions and procedures.

4- Developing the NEDRO Program to decrypt the encrypted data, especially secret data.

5- Encryption will be possible for databases by adding some procedures to the NEDRO Program.

6- NEDRO Program has ability to satisfy safe path for more than two sites. The advantage of this point is transferring one encrypted message to many places at the same time.

References

[1]- Jose Eduardo and Munive-Hernandez, "FPGA Implementation of AES Algorithm" –IEEE , Transactions on Computers, Vol. 51, Issue 12, pp. 1454-1459, 2011.

[2]- Jazib Frahim, Omar Santos, David White, "AES implementation on 8-bit microcontroller," Department of Electrical Engineering, University of California, Los Angeles, USA, September, 2009.

[3]- Carl Landwehr, A. Hevia and Y. Yin, "A practice-oriented treatment of pseudorandom number generators", Springer-Verlag, 2012.

[4]- Michael Luby and Charlie Rackoff. "A concrete security treatment of symmetric encryption: analysis of the DES modes of operation", In Proc. 38th Annual Symposium on Foundations of Computer Science, 2011.

[5]- Diffie Hellman "Privacy and Authentication: An Introduction to Cryptography**",** Proceedings of the IEEE, v. 67, n. 3, Mar 2010, pp. 397–427.

[6]-Subra Aile,Vivek.M.Chhabria,and T.G.Sankar babu, "International Conference on Emerging Applications of Information Technology": 978-0-7695-4329-1/11 © 2011.

[7]- Jose M. Granado-Criado , Miguel A.Vega-Rodrıguez, Juan M. Sanchez-Perez and Juan A. G ́omez-Pulido, "A new methodology to implement the AES algorithm using partial and dynamic reconfiguration", Integration, the VLSI Journal 43 (2010) 72-80.

[23]-Ritu Malik Rupali Syal "Performance Analysis of IP Security VPN "International Journal of Computer Applications (0975 – 8887) Volume 8– No.4, October 2010.

[19]-Shahnaz Kouhbor "Virtual Private Network and Point-to-Point Tunneling Protocol" OPNETWORK 2011, August (2011) 1-10,Paper number 1689.

[20]- Hiroaki, Y. Kamizuru, A. Honda, T. Hashimoto,K. Shimizu, and H.Yao, "Dynamic IP-VPN architecture for cloud computing", in nformation and Telecommunication Technologies (APSITT), 2010 8th Asia-Pacific Symposium on, 2010.

[11]-Gabrielle Demange, Myrna Wooders and Matthew Jackson, "FPGA Implementation of AES Algorithm" 10th IEEE International Conference on Advanced Learning Technologies,Vol.14,No.4, pp. 222-226, 2011.

[12]- Kader Hatem and Mohamed Abdual " Comparative Analysis of AES and RC4 Algorithms for Better Utilization " International Arab Journal of e-Technology, Vol. 2, No. 1, January 2006, pp.1-10.

[19]-Shahnaz Kouhbor "Virtual Private Network and Point-to-Point Tunneling Protocol" OPNETWORK 2011, August (2011) 1-10,Paper number 1689.

[20]- Hiroaki, Y. Kamizuru, A. Honda, T. Hashimoto,K. Shimizu, and H.Yao, "Dynamic IP-VPN architecture for cloud computing", in nformation and Telecommunication Technologies (APSITT), 2010 8th Asia-Pacific Symposium on, 2010.

[21]- Ahmadi, M.R.; Satti, M.M.; "A security solution for Wireless Local Area Network (WLAN)" IEEE Visualization 05, Minneapolis, USA, 2010.